/informatik & security /fh/// st.pölten

# How to secure IoT on the wireless physical layer

Henri Ruotsalainen

Institute of IT Security research, FH St Pölten

ITSecX 2018

# Project – Secret Key Generation for low power wide area networks

/informatik & security /fh III st.pölten

- **Co-operation partner**

Microtronics
We live M2M

*Austrian provider for M2M Communication Solutions*

- **Financing**

FFG

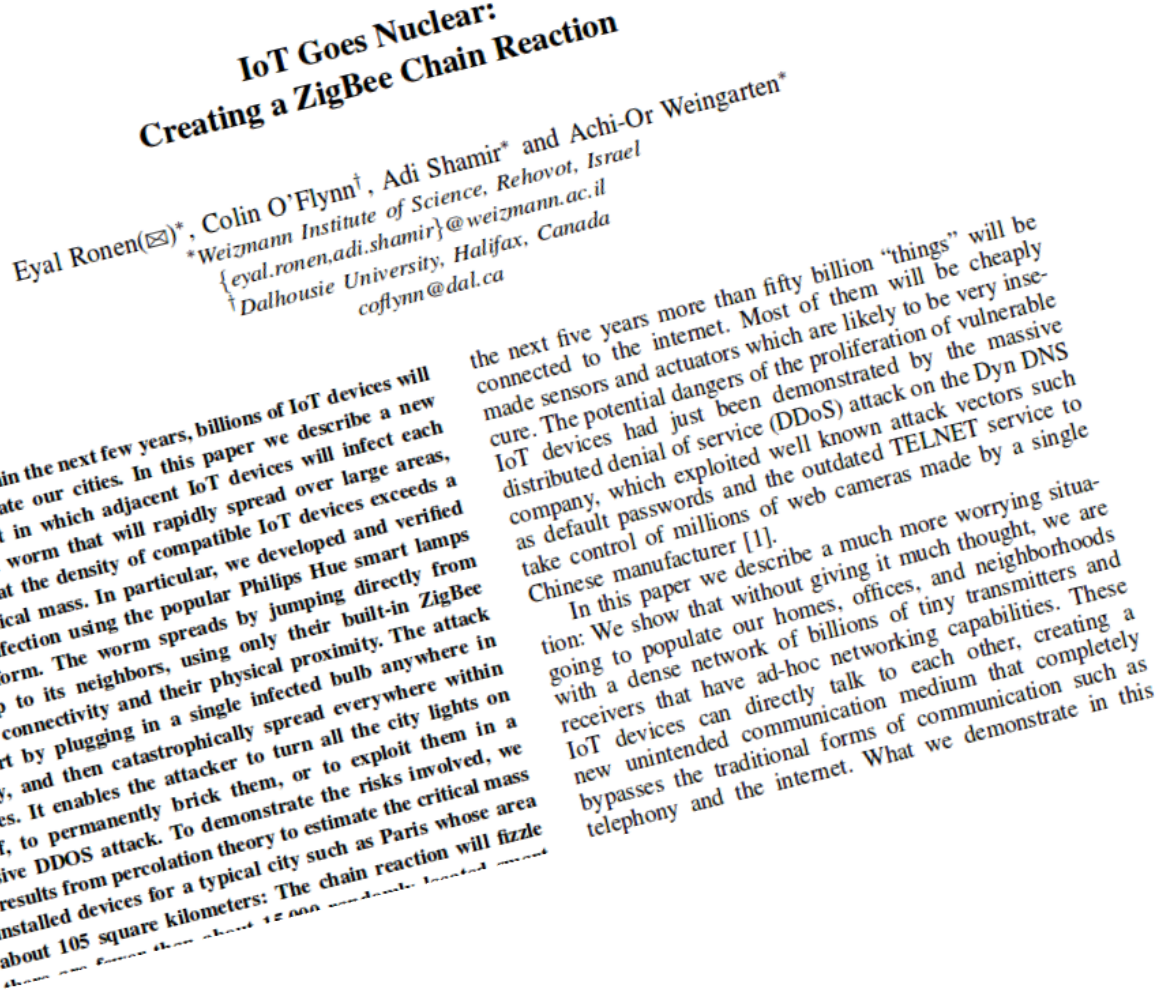
*Austrian Research Promotion Agency*

# Agenda

/informatik & security /fh/// st.pölten

- IoT physical layer attacks
- Wireless secret key agreement with LoRa signaling
- Experimental results
- Conclusions and challenges ahead

# IoT attacks



**IoT Goes Nuclear:**
**Creating a ZigBee Chain Reaction**

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*
*Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
†Dalhousie University, Halifax, Canada
coflynn@dal.ca

*Abstract*—Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will rapidly spread over large areas, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes. It enables the attacker to turn all the city lights on or off, to permanently brick them, or to exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizzle

the next five years more than fifty billion "things" will be connected to the internet. Most of them will be cheaply made sensors and actuators which are likely to be very insecure. The potential dangers of the proliferation of vulnerable IoT devices had just been demonstrated by the massive distributed denial of service (DDoS) attack on the Dyn DNS company, which exploited well known attack vectors such as default passwords and the outdated TELNET service to take control of millions of web cameras made by a single Chinese manufacturer [1].

In this paper we describe a much more worrying situation: We show that without giving it much thought, we are going to populate our homes, offices, and neighborhoods with a dense network of billions of tiny transmitters and receivers that have ad-hoc networking capabilities. These IoT devices can directly talk to each other, creating a new unintended communication medium that completely bypasses the traditional forms of communication such as telephony and the internet. What we demonstrate in this

# IoT attacks



"We managed to deduce all the secret cryptographic elements used by Philips (such as IVand key) within a few days, using novel side channel attacks that used only cheap and easily obtained equipment costing a few hundred dollars, and without physically extracting them from their secure memory. Once we obtained these secret values, we could create any new firmware and upload it into any Philips Hue lamp"

"IoT goes Nuclear : Creating a Zigbee Chain reaction", E. Ronen & al., IEEE Symposium for Security & Privacy 2017

# IoT attacks



"**We managed to deduce all the secret cryptographic elements** used by Philips (such as IVand key) **within a few days**, using novel side channel attacks that used only **cheap and easily** obtained equipment costing a few hundred dollars, and **without physically extracting them** from their secure memory. **Once we obtained these secret values, we could create any new firmware and upload it into any Philips Hue lamp**"

"IoT goes Nuclear : Creating a Zigbee Chain reaction", E. Ronen & al., IEEE Symposium for Security & Privacy 2017

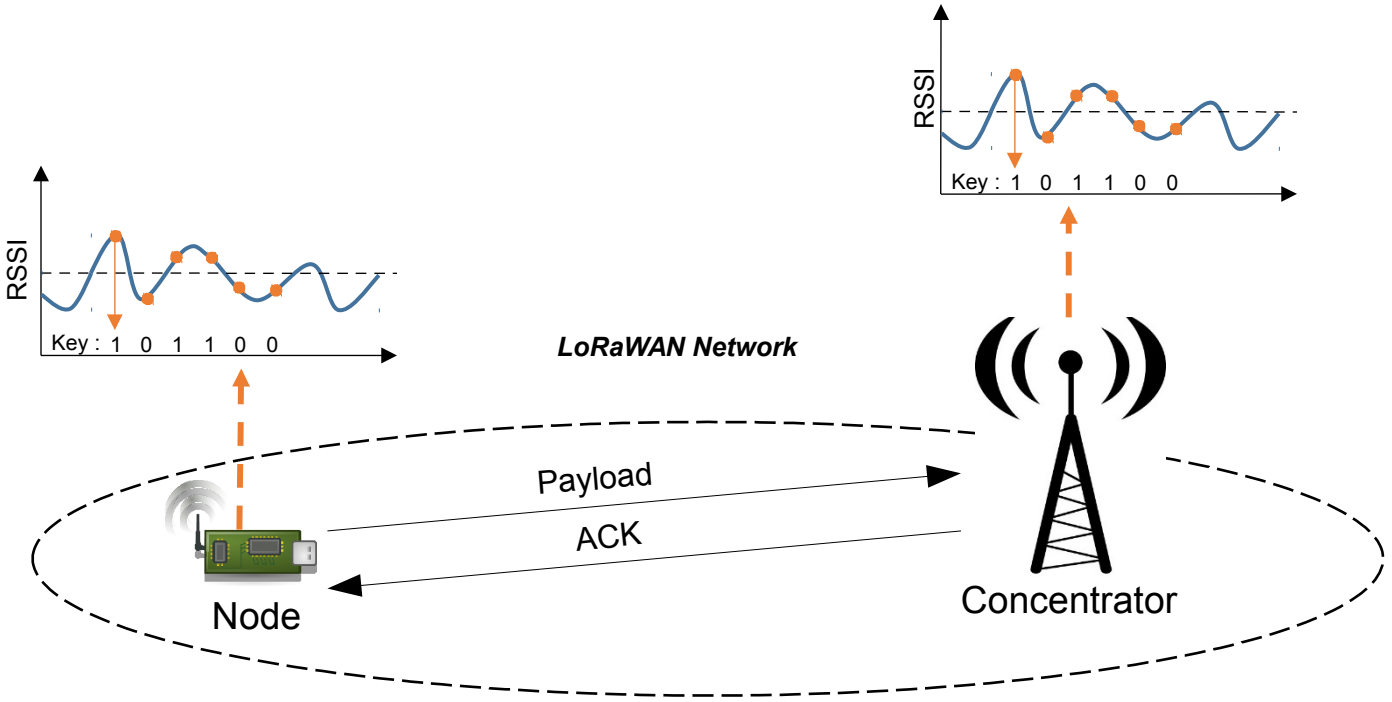
# IoT attacks

*Poor key management on embedded systems may lead to*

- *Power black-outs while an attacker controls synchronously thousands of mains connected devices*
- *“more calls to ÖAMTC” as an attacker has poisoned the control system of a car*
- *Exotic DoS attacks as an attacker Jams ISM bands with captured IoT devices*

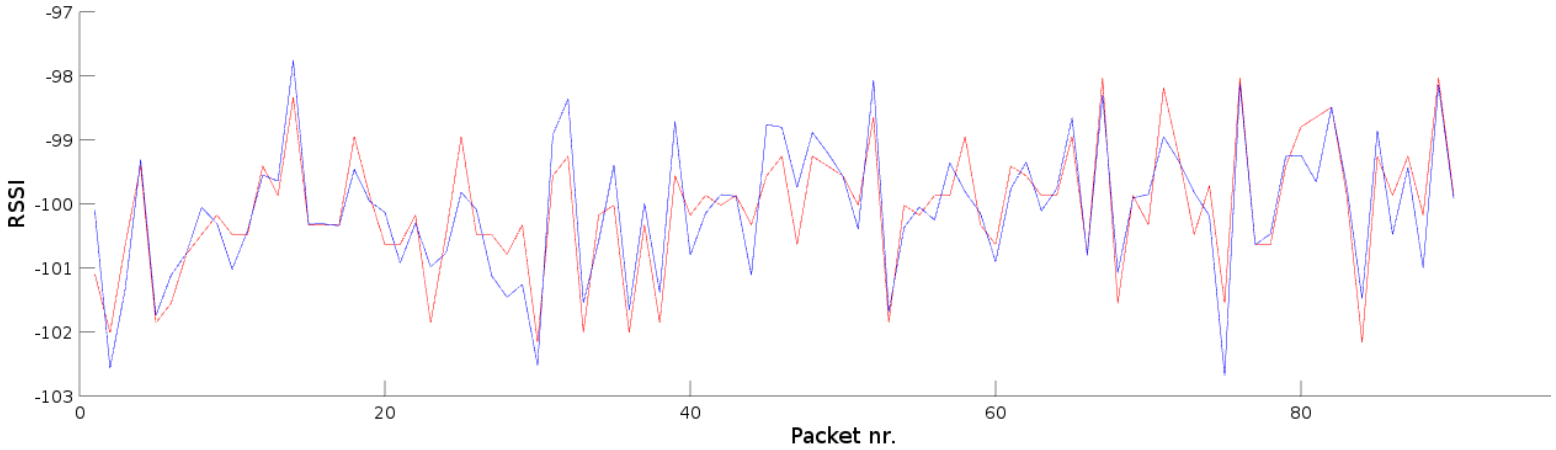
# Wireless secret key agreement

- Randomness of the wireless channel in bi-directional communication can be converted into secret keys



# Wireless secret key agreement

- Illustration of symmetric RSSI values at Alice (LoRa Node) and Bob (LoRa Node)




Generated bit streams (Alice Bob)

000110111

000110111

# Wireless secret key agreement

/informatik & security /fh/// st.pölten

***Advantages***

- Survives quantum computer attacks
- Wireless infrastructure is (almost) already there
- Key agreement algorithms are light-weight

***Challenges***

- *Secret key agreement in LPWAN (← our focus!)*
- Practical implementations

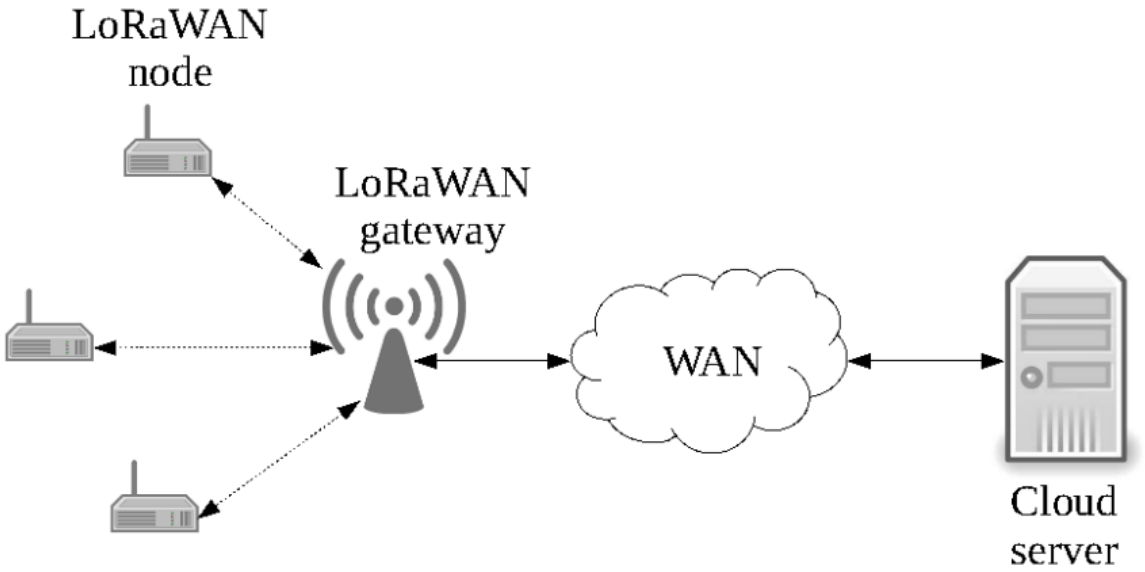
# LoRa technology

/informatik & security /fh/// st.pölten

- Wireless physical layer targetted at LPWAN applications
- Typical data rates in kb/s
- Based on chirp-spread spectrum modulation
- Optimized for low power and high range (> 10km)
- Operates on unlicenced ISM bands

# LoRaWAN

- Wireless standard defining MAC & Network structure of LPWAN
- Star-of-stars topology
- Three classes of operation: Class-A,B & C

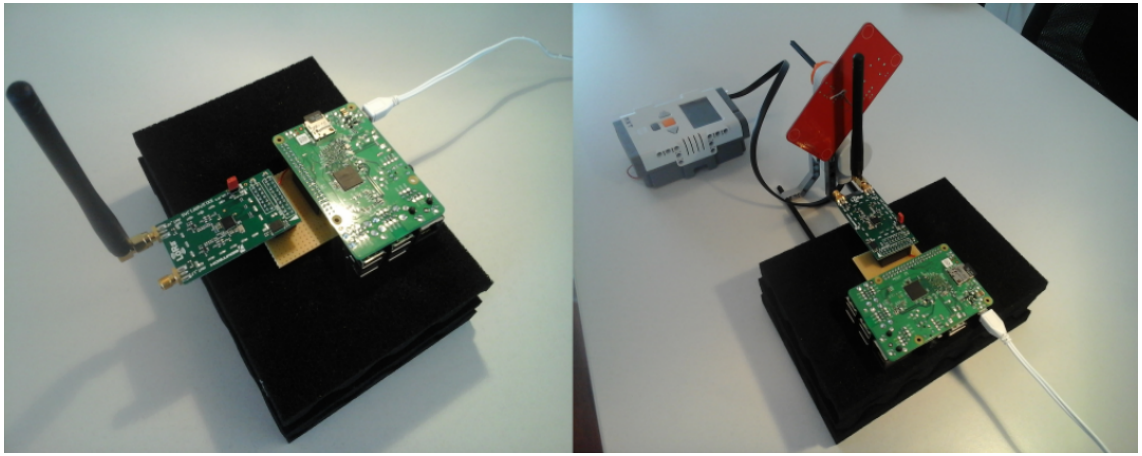


# Experimental results



***Measurement equipment:***

- 2 x Raspberry PI with Semtech eval board for SX1276 LoRa modem
- PCB mounted on stepper motor



# Experimental results

/informatik & security /fh/// st.pölten

***Figure of merits***

- Correlation
- Key agreement&disagreement rate (KAR/KDR)
- Keys per measurement (KPM)
- Approximate entropy (AE)

***Measured values***

- Mean value of channel RSSI (rRSSI)
- Packet RSSI (pRSSI)

# Experimental results

/informatik & security /fh/// st.pölten

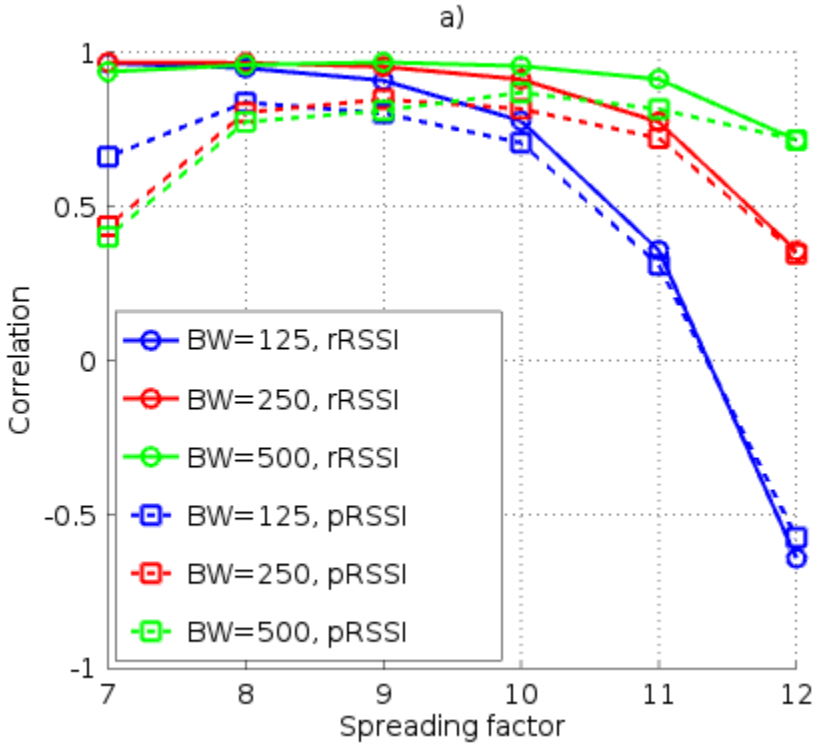
***Measurement scenarios:***

- 1. „LoRa Parameters“
- 2. „(dynamic) Deep in-building penetration“
- 3. „Static in-door“
- 4. „Static out-door“
- 5. „Eavesdropping attacks“

# Experimental results

/informatik & security /fh/// st.pölten

***Scenario 1.*** „LoRa parameters“

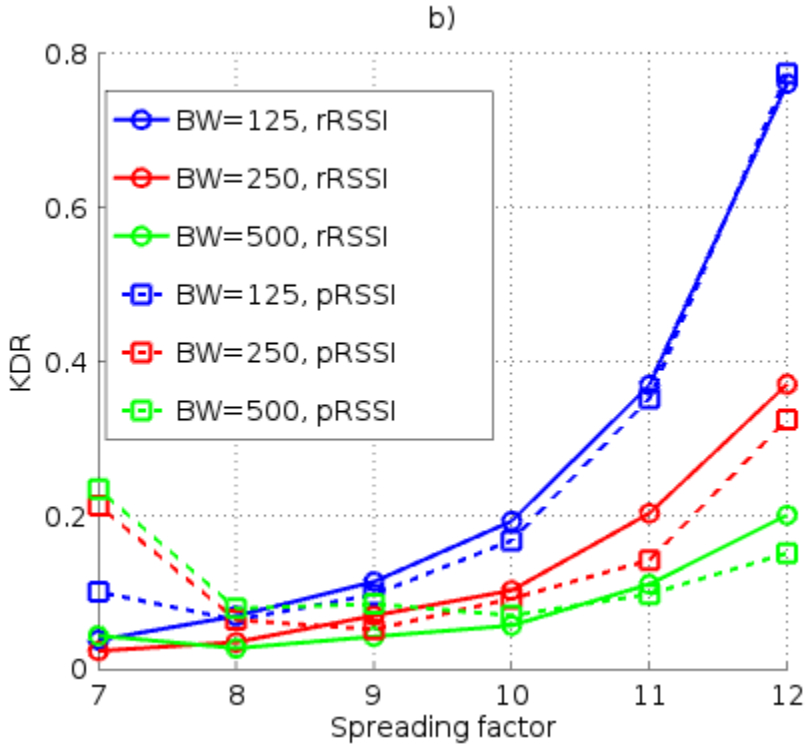


# Experimental results

/informatik & security /fh/// st.pölten

***Scenario 1.*** „LoRa parameters“

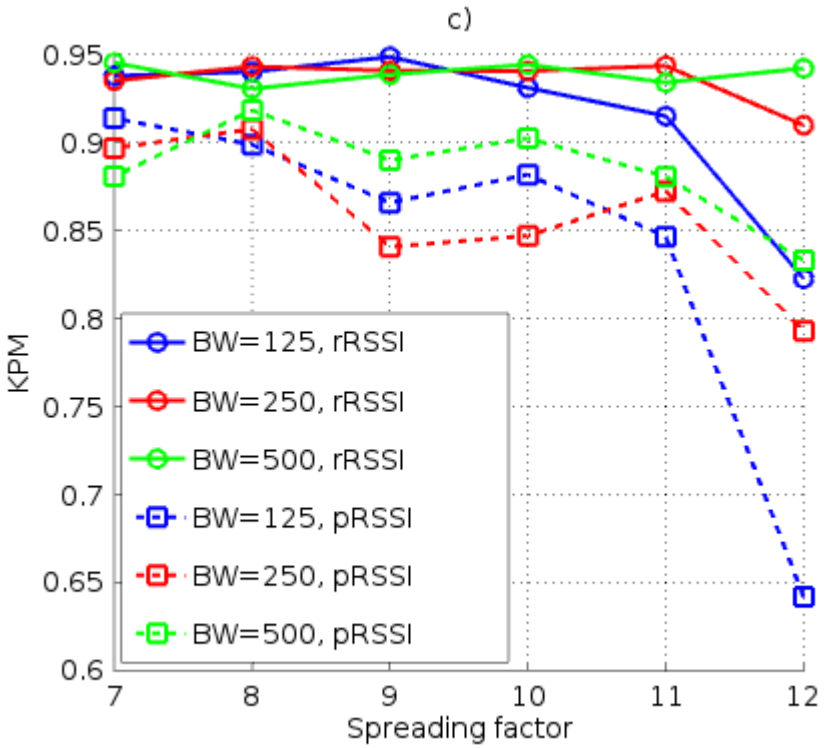
- Result: *For low bandwidth & high SF, channel probing delay becomes prohibitively high, which increases KDR*



# Experimental results

***Scenario 1.*** „LoRa parameters“

- Result: *rRSSI performs overally better*



# Experimental results



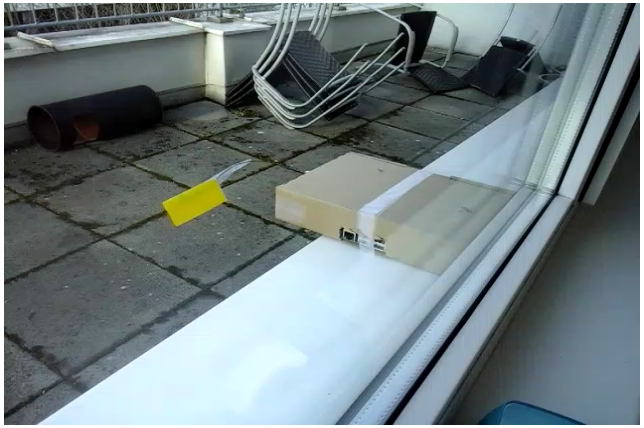
***Scenarios 2-4*** „Deep building penetration/static indoor/static outdoor“

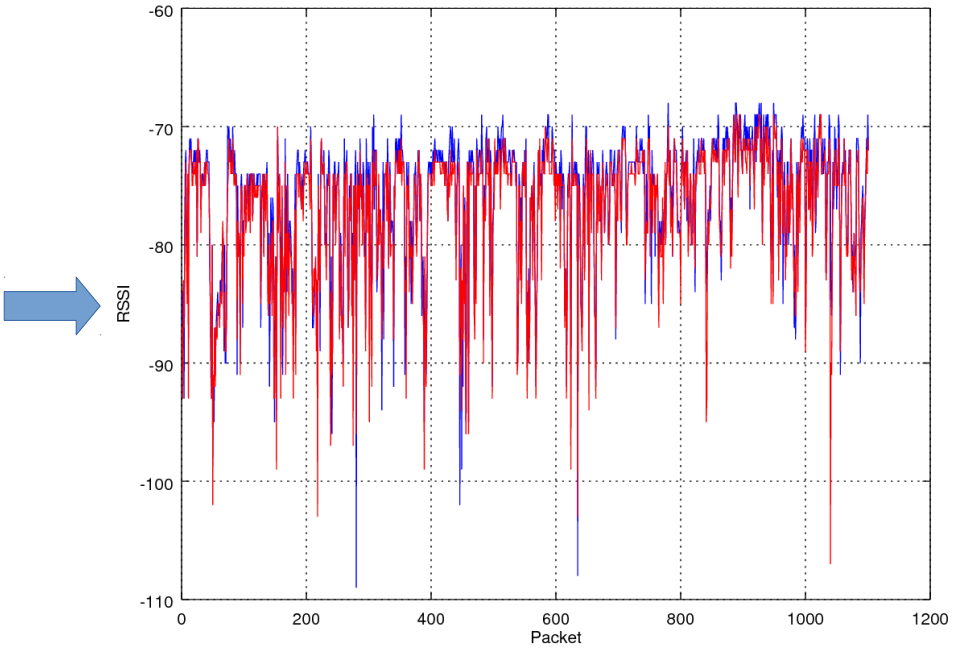
- Result: *A flexible antenna leads potentially to stronger keys in static outdoor communication scenarios*

| Scen. | r*AE | rKPM | rKDR | p*AE | pKPM | pKDR |
|---|---|---|---|---|---|---|
| III | 0.237 | 61% | 12% | 0.047 | 61% | 14% |
| IV | 0.071 | 55% | 8% | 0.008 | 65% | 29% |
| V | 0.719 | 60% | 8% | 0.705 | 59% | 14% |

# Experimental results

***Scenarios 4*** „Static outdoor“, Converting wind into secret keys...





# Experimental results

/informatik & security /fh/// st.pölten

***Scenarios 5*** „Eavesdropping attacks“

- Result: *An eavesdropper attack might become detectable from channel probing statistics*

| Distance | KAR A-B | KAR A-E | KAR B-E | rCorr. |
|---|---|---|---|---|
| 2m | 89% | 52% | 47% | 0.93 |
| 15cm | 85% | 56% | 56% | 0.93 |
| 0cm | 85% | 71% | 70% | 0.85 |

# Conclusions

/informatik & security /fh/// st.pölten

- Wireless Secret Key Agreement implemented first time for LoRa physical layer
- RSSI Channel probing methods available in LoRa modems were investigated
- Presented key agreement scheme applies directly to LoRaWAN Class-C

*Experimental results indicate that:*

- Direct channel RSSI probing leads to better key agreement
- High channel probing times might limit high range key agreement

# Challenges ahead

- Secret key agreement for LoRaWAN Class-A (low energy) with delayed downlink communication windows
- Secret key agreement in real-world LoRaWAN networks with packet collisions
- Secret key agreement over several km with LoRaWAN (noisy measurements)

# Thank you for your attention!
# Questions?